PROMISE®
TECHNOLOGY, INC.

VTRAK S3000
Snapshot Agents
User Manual

Version 1.0

Copyright

© 2010 PROMISE Technology, Inc. All Rights Reserved. PROMISE, the PROMISE logo, VTrak, SmartStor, SuperTrak, FastTrak, VessRAID, Vess, PerfectPATH, PerfectRAID, SATA150, ULTRA133 VTrak S3000, BackTrak, HyperCache, HyperCache-R, HyperCache-W, DeltaScan and GreenRAID are registered or pending trademarks of PROMISE Technology, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners. Information regarding products, services and offerings may be superseded by subsequent documents and are subject to change without notice. For the latest information and specifications regarding PROMISE Technology, Inc. and any of its offerings or services, please contact your local PROMISE office or the corporate headquarters. Visit www.promise.com for more information on PROMISE products.

Important data protection information

You should back up all data before installing any drive controller or storage peripheral. PROMISE Technology is not responsible for any loss of data resulting from the use, disuse or misuse of this or any other PROMISE Technology product.

Notice

Although PROMISE Technology has attempted to ensure the accuracy of the content of this manual, it is possible that this document may contain technical inaccuracies, typographical, or other errors. PROMISE Technology assumes no liability for any error in this publication, and for damages, whether direct, indirect, incidental, consequential or otherwise, that may result from such error, including, but not limited to loss of data or profits.

PROMISE Technology provides this publication “as is” without warranty of any kind, either express or implied, including, but not limited to implied warranties of merchantability or fitness for a particular purpose.

The published information in the manual is subject to change without notice. PROMISE Technology reserves the right to make changes in the product design, layout, and driver revisions without notification to its users.

This version of the *Product Manual* supersedes all previous versions.

Recommendations

In this *User Manual*, the appearance of products made by other companies, including but not limited to software, servers, and disk drives, is for the purpose of illustration and explanation only. PROMISE Technology does not recommend, endorse, prefer, or support any product made by another manufacturer.

Contents

Chapter 1: Introduction 1
Diagnostics 1
X-ray 1
Log files 1
Installation Overview 2

Chapter 2: Snapshot Agent for Microsoft Exchange 3
Supported Versions 3
Before you Install the Snapshot Agent 3
Installing the Snapshot Agent 4
Silent installation 4
Configuring the Snapshot Agent 4
Running the Snapshot Agent 4
Confirming Snapshot Status 4
Purging the Log Utility 5
Removing Snapshot Agent Software 6

Chapter 3: Snapshot Agent for Oracle 7
Supported Versions 7
File Systems Support 7
Installation on Windows 7
Silent Installation 8
Installing on Oracle 11 8
Installing on Oracle 10 8
Installing on Oracle 9 8
Installing on Oracle 8 8
Configuring the Snapshot Agent on Windows 9
Configuring ASM disks 11
Configuring the Oracle Listener 11
Installation on Linux 12
Configuring the Snapshot Agent on Linux . 13
Turning On Oracle Archive Logging 14
Running the Snapshot Agent 14
Confirming Snapshot Status 15
Removing Snapshot Agent 15
Windows 15
Protecting and Recovering Oracle Databases . 15
Database Design with Virtual Devices 15
Physical location of the tablespaces . . . 15
Fault tolerance and performance considerations 16
Free disk space considerations 16
Using groups 16
Data Backup and Protection Scenarios . . . 16
Snapshot 16
Snapshot Copy 16
SnapshotView 17
Replication 17
Snapshot Rollback 17
Complete backup using a SnapshotView or Snapshot Copy 17

Chapter 3: Snapshot Agent for Oracle, cont.
Protecting and Recovering Oracle Databases, cont.
Recovery Scenarios 17
Disk Failure 17
User Failure 18
Operator failure 18
Restoring Backed-up Oracle Databases . . . 18
Automatic recovery 19
Manual recovery 19

Chapter 4: Snapshot Agent for Microsoft® SQL Server 21
Supported Versions 21
Installation 21
Silent installation 21
Configuring the Snapshot Agent 22
Advanced Configuration 25
Transaction Log Backups 25
Command line utility 26
Trace Log 26
Run the Snapshot Agent 27
Confirm Snapshot Status 27
Remove Snapshot Agent Software 28

Chapter 5: Snapshot Agent for MySQL 29
Supported versions 29
Installation 29
Configuring the Snapshot Agent 29
Running the Snapshot Agent 29
Confirming Snapshot Status 29
Removing Snapshot Agent software 30

Chapter 6: Snapshot Agent for VSS 31
About Microsoft VSS 31
Snapshot Agent for VSS 31
Supported Versions 31
Snapshot Process 31
Supported Writers 32
Microsoft® Exchange 2010/Exchange 2007 32
Microsoft® SQL 2008 32
Microsoft® Hyper-V 32
Microsoft® Active Directory 2008/Microsoft® Active Directory 2008 R2 32
Storage Configuration Guidelines 32
Installating the Snapshot Agent 32
Silent Install 33
Configuring the Snapshot Agent 33
Performing a Full Backup 33
Running Database or Application Verification 34
Advanced Options 34
Batch File Options 35
Running the Snapshot Agent 35
History and Event Logs 35
Removing Snapshot Agent Software 35

Chapter 7: Snapshot Agent for File Systems . . . 37
Supported Versions 37
Installation on Linux 37
Installation on Windows 37
Silent Installation 38
Configuring the Snapshot Agent on Windows . . 38
Running the File System Agent 38
Confirming Snapshot Status 38
Removing the Snapshot Agent Software 38

Index 39

Chapter 1: Introduction

- Diagnostics (page 1)
- Installation Overview (page 2)

Today’s businesses put increasing demands on information and databases, resulting in the need for 24x7 availability and high performance. However, ever-growing capacity presents significant challenges in meeting these high availability and performance requirements.

One of the most important issues identified by system administrators is the amount of time associated with backup, and more importantly, recovery. Prolonged downtime, sometimes in the range of hours or days, is often experienced while recovering corrupted or lost data.

Because it takes a significant amount of time to copy large amounts of data to tape or other media, the source data can change before the copying is complete. Therefore, the data written to tape represents changes over a period of time and does not have *point-in-time* referential integrity. There is no guarantee that the data written to tape can be meaningfully restored.

Snapshot Agents protect databases, messaging systems, and file systems with full point-in-time consistency while allowing full speed, non-stop access to the data. Working together or independently, Snapshot Agents ensure that active data is protected in an enterprise environment with a shrinking backup-window. Complete data and transactional integrity is attained through a robust and automated process that safely and reliably takes snapshots of data for point-in-time copy purposes, third-party backup applications, and disaster recovery planning.

Snapshot Agents work seamlessly with all of these options:

- Replication
- Snapshot
- Snapshot Copy
- BackTrak

These options are based on a built-in snapshot engine. The Snapshot Agents ensure that the resulting copy of data has both point-in-time consistency and transactional integrity. This feature can save many hours of valuable time in the case of a disaster.

Using the Replication option with the Snapshot Agents provides an easy method of maintaining replicated data for off-host processing. Backups be performed on the replica. Also, data can be changed for:

- Testing
- What-if analysis
- Training

Systems can be resynchronized quickly and easily with no impact to the production server.

The Snapshot Agents help make many data management tasks possible, such as backup or replicating data to an off-site location, thus meeting the requirements of high availability and high performance.

Diagnostics

X-ray

All Windows-based Snapshot Agents include an X-ray feature which allows you to get X-ray information from your storage servers for diagnostic purposes. Each X-ray contains technical information about the server, such as server messages and a snapshot of the server's current configuration and environment.

To capture an X-ray:

1. Launch the configuration tool, and
2. From the **About** menu, select **Take X-ray**.

This generates a **.cab** file that can be sent to Technical Support for diagnostics.

Log files

Some Agents write to log files automatically but all must be configured to write detailed information to the trace log. To turn on the agent configuration program for a Snapshot Agent, left-click in the top left corner to produce a menu. Then select settings from the menu and check the **Set Agent trace on** box.

Some Agents may have a numerical entry next to the *Set Agent trace on* parameter (for example 0-10). The higher the number, the more detailed the information.

- 0 – Errors
- 1-3 – Usually informational messages
- 4-10 – Detailed information for technical support

The additional information displays in the log after the next snapshot is taken. Refer to each Snapshot Agent chapter for specific log file information.

- “Chapter 2: Snapshot Agent for Microsoft® Exchange” on page 3
- “Chapter 3: Snapshot Agent for Oracle®” on page 7
- “Chapter 4: Snapshot Agent for Microsoft® SQL Server” on page 21
- “Chapter 5: Snapshot Agent for MySQL” on page 29
- “Chapter 6: Snapshot Agent for VSS” on page 31
- “Chapter 7: Snapshot Agent for File Systems” on page 37

Installation Overview

In order to install a Snapshot Agent as part of an inband solution, you must follow the steps below.

1. Install and configure an iSCSI initiator or Fibre Channel HBA on your client machine.

   The client machine must connect to your storage server.

   See the *VTrak S3000 Quick Start Guide* for more information.

2. IMA and SAN Client software enable the client machine to access storage server resources.

   IMA must be installed on each Windows client machine. On Windows machines, SAN Disk Manager manages and configures the client machine. It installs automatically with IMA.

   SAN Client software must be installed on each Linux client machine.

   If SDM/IMA is not detected when Snapshot Agent installation begins, an error message displays.

   See the *VTrak S3000 Server User Manual* for more information.

3. Create SAN Resources for your database/messaging system files.

   Determine how many SAN Resources to create. Typically, databases require that the data files be on a separate disk from the log files. Determine how many disks are needed for your database or messaging system. Then create SAN Resources for each one.

   See the *VTrak S3000 Server User Manual* for more information.

4. Create a snapshot group for your SAN Resources.

   Snapshot groups ensure transactional integrity for database and messaging files that reside on multiple disks. Snapshots for all resources in a group are taken at the same time whenever a snapshot is triggered.

   See the *VTrak S3000 Server User Manual* for more information.

5. Migrate the database and messaging system files you want to protect with a Snapshot Agent to the VTrak S3000 server-managed disk.
6. Install your *database/application* Snapshot Agent.

   See the appropriate chapter in this manual for more information.

7. Install the *appropriate filesystem* Snapshot Agent.

Chapter 2: Snapshot Agent for Microsoft® Exchange

- Supported Versions (page 3)
- Before you Install the Snapshot Agent (page 3)
- Installing the Snapshot Agent (page 4)
- Configuring the Snapshot Agent (page 4)
- Running the Snapshot Agent (page 4)
- Confirming Snapshot Status (page 4)
- Purging the Log Utility (page 5)
- Removing Snapshot Agent Software (page 6)

Important

If you are using Microsoft Exchange 2010, you must use “Chapter 6: Snapshot Agent for VSS” on page 31, since Exchange 2010 supports only VSS snapshots.

The Snapshot Agent for Microsoft Exchange protects Exchange databases by ensuring the transactional integrity of snapshots.

Prior to starting the snapshot process, a request is sent to the application server running the Snapshot Agent for Microsoft Exchange. The Agent briefly puts the database into backup mode and notifies the server that the snapshot can be performed. Once the snapshot has completed, the server notifies the application server and the Agent takes the database out of backup mode.

Using backup software, a backup of the snapshot image can be performed at high speed while Microsoft Exchange operates in normal mode. While the backup software is reading data from the snapshot image, changes that occur to the database will not affect what gets written. Users are always able to see the database with full access at all times while the backup software sees a stable, read-only snapshot image of the database taken an instant before the backup began.

Supported Versions

The Snapshot Agent for Microsoft Exchange is supported for Windows Enterprise Server platforms. For specific version information, refer to the Certification Matrix on the www.promise.com website.

Important

You can only have one Exchange Virtual Server active per node. Therefore, you should not have a snapshot group with multiple Virtual Servers on the same node.

Before you Install the Snapshot Agent

Before installing the Snapshot Agent, you must use your Exchange System Manager to move the following files and databases to VTrak S3000 server-managed disk.

The following should be on the same disk:

- Exchange log
- System path

The following should be together on a separate disk from the log file:

- Exchange database
- Exchange streaming database

Important

Recovery is very difficult if you do not adhere to these guidelines.

Installing the Snapshot Agent

Installation of the Snapshot Agent has the following requirements:

- Before you install the Snapshot Agent, you must install PROMISE SAN Disk Manager (SDM/IMA) on the same machine. If SDM/IMA is not detected when Snapshot Agent installation begins, an error message displays. Cancel the procedure, install SDM/IMA, and then repeat Snapshot Agent installation.
- The Snapshot Agent must be installed on the same machine where the Exchange Server is running.
- Your Exchange Server must be started before installing the agent.
- You must be an administrator or have administrator privileges in order to install the Snapshot Agent.

To install:

1. Launch installation from the installation media.
2. When prompted, enter your license key code.

   The Snapshot Agent license must be registered with PROMISE.

   - If your computer has an Internet connection, the license is activated as soon as you enter your key code and click the **Next** button.
   - If your Internet connection is temporarily down, your license activates automatically the next time the Snapshot Agent is started and your Internet connection is working.
   - If your computer has no Internet connection, you must perform an offline activation.

   You have 30 days to activate your license so that you can continue to use the Agent.
3. When you are done, click **Finish**.

   The Agent installs to the same directory as SDM/IMA.

Silent installation

The Snapshot Agent provides the ability to perform a silent install. A silent install does not require any interaction during the installation process.

In order to install the Snapshot Agent in silent mode, run *setup /s* or *setupsilent.bat*.

Configuring the Snapshot Agent

By default, no configuration of the Snapshot Agent is required. However, if you are using a service-enabled device (SED) and you have preserved the physical device's inquiry string (this is set when you create the SED in the Console), you must modify the **ExAgent.ini** file that is created under the directory when the Snapshot Agent is installed. In the **ExAgent.ini** file, you must use the DriveOverride option to specify the drive letters to which the SED is mounted.

For example: **DriveOverride=E:;** or **DriveOverride=E:;F:;**

Also, if you want to send snapshot results to a third-party management system, you must use the Exchange configuration utility to enter the *User Name* and *Password* of a member of the local administrators group. This user account does not need permission from the Exchange Administrator; it is only used to run the pre-script (**exchpre.bat)** and post-script (**exchpost.bat**) that are saved in the IMA installation folder. You need not run these scripts unless you want to send Snapshot results to a third-party management system.

After the installation completes, the configuration utility launches automatically.

Running the Snapshot Agent

The Snapshot Agent triggers automatically any time a snapshot operation occurs on the Microsoft Exchange drive.

To test the Snapshot Agent, you can perform a Snapshot Copy of a virtual drive from the Console.

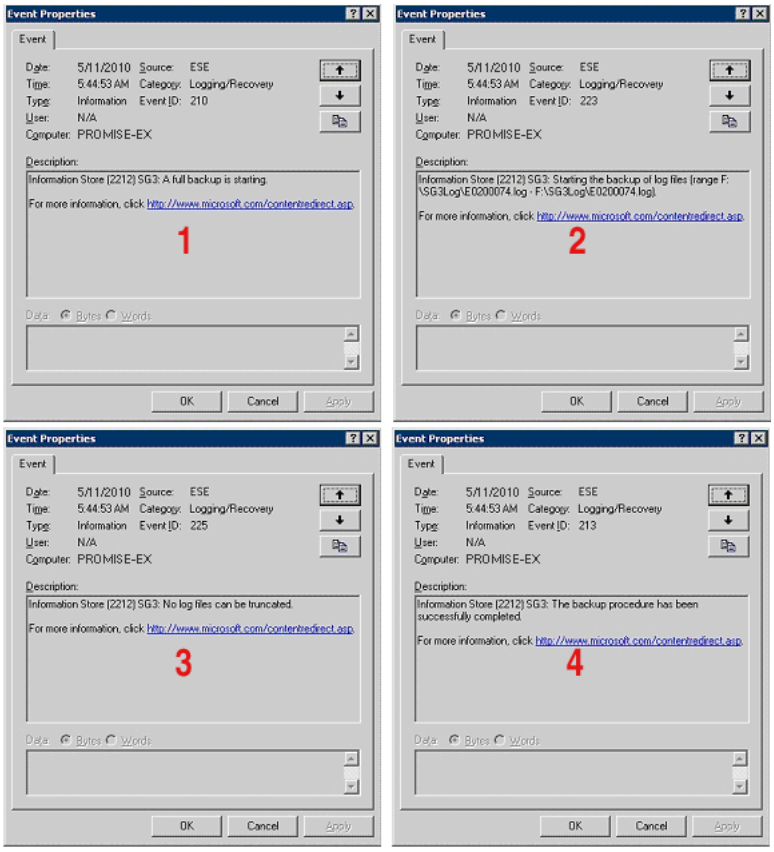
Confirming Snapshot Status

To confirm the Exchange snapshot process, you can check the Windows Event log. The Snapshot Agent will send the backup command to each storage group on the protected disk. You can find these logs after the *appctrl* event:

1. The Snapshot Agent sends the full backup command to the storage group and then Exchange Extensible Storage Engine (ESE) starts the full backup process.
2. Exchange ESE checks the log files and the checkpoint.

3. Exchange ESE processes the log files. The Snapshot Agent does not request to truncate the log to affect other Exchange backup process.

   Exchange ESE completes the backup process on a storage group. You may see the same process on another storage group.



Purging the Log Utility

If you are using the Snapshot Agent for MS Exchange to protect your Exchange environment but do not have third-party backup software to help purge the Exchange log files, you can use this utility to clean up Exchange log files.

Before you run the **ISPurgeExLog** utility, make sure the latest snapshot was taken successfully by checking the Windows Application Event Log. You can also dump the MS Exchange Checkpoint file using **ESEUTIL.EXE** and check the timestamp of **FullBackup Time** to view the record of the last snapshot date and time.

The Microsoft Exchange log file is generated based on each “Exchange Storage Group.” You must run log purge against log files on each Exchange Storage Group. You can schedule a batch job with the following command inside the batch file.

For Microsoft Exchange 2003:

ISPurgeExLog "F:\Exchsrvr\System\E00.chk" "F:\Exchsrvr\log" –v

For Microsoft Exchange 2007:

ISPurgeExLog64 "F:\Exchsrvr\System\E00.chk" "F:\Exchsrvr\log" –v

You must specify the location of checkpoint file and log directory as a parameter.

ISPurgeExLog "<Checkpoint File>" "<Exchange Log directory>" [Options]

Option	Description
-b#hour	#hour is number of hours before the recorded checkpoint time, maximum 96 hours. (examples: -b04, -b16, default is -b24).
-c	Use last checkpoint log file date time if it is earlier than last full backup date time.
-hHour	Hour is from 00 to 23(examples: -h04, -h16). Execute purge only when run within specific hour (hh:00-hh:59)
-i	Ignore last full backup timestamp on CCR passive node. Works with -c option.
-p	Preview the purge list without actually deleting the logs.
-r"reportFileName”	Additional Report File Generated.
-s"StorageGroupName"	Storage Group Name in Report File.
-v	Verbose mode.

PROMISE recommends that you run the purge utility once a day, maintaining 24 hours of log files after each log purge. After the purge, you can examine the log file directory and make sure older log files are deleted. An **ISPurge.log** file is created containing the history of each **ISPurgeExLog** execution.

Removing Snapshot Agent Software

You can use **Add/Remove Programs** from the Control Panel or:

1. Insert the installation media.
2. Choose **Install Products** > **Install Snapshot Agents** > I**nstall Snapshot Agent for Microsoft Exchange** and follow the on-screen instructions to uninstall the Snapshot Agent.

Chapter 3: Snapshot Agent for Oracle®

- Supported Versions (page 7)
- Installation on Windows (page 7)
- Turning On Oracle Archive Logging (page 14)
- Running the Snapshot Agent (page 14)
- Confirming Snapshot Status (page 15)
- Removing Snapshot Agent (page 15)
- Protecting and Recovering Oracle Databases (page 15)

The Snapshot Agent for Oracle protects Oracle databases with full point-in-time consistency while still allowing full speed, non-stop access to the databases.

Prior to starting the snapshot process, a request is sent to the application server running the Snapshot Agent for Oracle. The Agent places the Oracle database in *backup* mode and notifies the server that the snapshot can be performed. While in *backup* mode, the database is *frozen* and Oracle sends all new incoming data to the Oracle *online redo logs*. Once the snapshot has completed, the server notifies the application server and the Agent places the database back into normal mode, synchronizing all data back to the database.

Using backup software, a back up of the snapshot image can be performed at high speed while Oracle operates in normal mode. Because the contents of the snapshot image are guaranteed never to change, what is backed up is consistent, ensuring transactional integrity. While the backup software is reading data from the snapshot image, changes that occur to the database will not affect what gets written. Users are always able to see the database with full access at all times while the backup software sees a stable, read-only snapshot image of the database taken an instant before the backup began.

Supported Versions

The Snapshot Agent for Oracle is supported for the following platforms. For specific version information, refer to the Certification Matrix on the PROMISE website.

- Red Hat Enterprise Linux
- Red Hat Linux Advanced Server
- SUSE Linux
- Windows

Important

If a raw device is used for the Oracle database, you must store the Oracle control file on another virtual disk, which should be in the same group as the raw device's virtual disk. Otherwise, snapshots of the raw device database may be inconsistent.

File Systems Support

The Snapshot Agent for Oracle supports the following file systems:

- **ASM** – Automated Storage Management. The disks are raw LUNs.
- **OCFS** – Oracle Cluster File System.

Installation on Windows

Installation of the Snapshot Agent has the following requirements:

- Install PROMISE SAN Disk Manager (SDM/IMA) first, then install the Snapshot Agent.

  If SDM/IMA is not detected when Snapshot Agent installation begins, an error message displays. Cancel the procedure, install SDM/IMA, and then repeat Snapshot Agent installation.
- Start your Oracle database first, then install the agent.
- You must be an administrator or have administrator privileges in order to install the Snapshot Agent.
- Turn on Oracle archive logging.
- Oracle 8i only – Make sure the required library **%ORA_HOME%/precompile/lib/orasql8.LIB** is present in the system.

  If the file is not present, reinstall the Oracle client software and select **Programmer** as the installation type.

To install Snapshot Agent on Windows:

1. Launch installation from the installation media.
2. Select which versions of Oracle you are using.

   You must have a separate license for each.
3. When prompted, enter your license key code.

   The Snapshot Agent license must be registered with PROMISE.

   - If your computer has an Internet connection, the license is activated as soon as you enter your key code and click the **Next** button.
   - If your Internet connection is temporarily down, your license activates automatically the next time the Snapshot Agent is started and your Internet connection is working.
   - If your computer has no Internet connection, you must perform an offline activation. .

   You have 30 days to activate your license so that you can continue to use the Agent.
4. When you done, click the **Finish** button.

   The Agent installs to the same directory as SDM/IMA.

Silent Installation

The Snapshot Agent provides the ability to perform a silent install. A silent install does not require any interaction during the installation process.

The Snapshot Agent installation package offers support for Oracle 8, 9, 10, and 11. Snapshot Agent for Oracle 11 is the default package.

Installing on Oracle 11

To install the Snapshot Agent for Oracle 11 in silent mode, run the commands

setup /s or **setupsilent.bat**

Installing on Oracle 10

To install the Snapshot Agent for Oracle 10 in silent mode:

1. Copy **setup10.iss** to **setup.iss**.
2. Run the commands

   setup /s or **setupsilent.bat**.

Important

If your Oracle server is running a 64-bit operating system, you must make the same changes in the AMD64 directory.

Installing on Oracle 9

To install the Snapshot Agent for Oracle 9 in silent mode:

1. Copy **setup9.iss** to **setup.iss**
2. Run the commands

   setup /s or **setupsilent.bat**

Important

If your Oracle server is running a 64-bit operating system, you must make the same changes in the AMD64 directory.

Installing on Oracle 8

To install the Snapshot Agent for Oracle 8 in silent mode:

1. Copy **setup8.iss** to **setup.iss**
2. Run the commands

   setup /s or **setupsilent.bat**

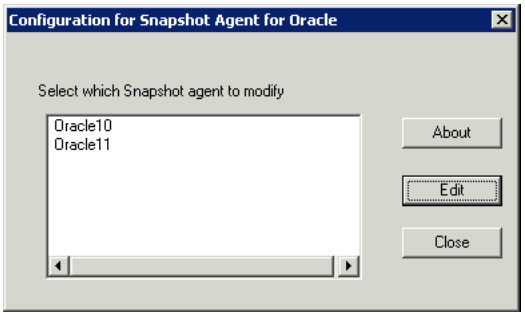
Important

If your Oracle server is running a 64-bit operating system, you must make the same changes in the AMD64 directory.

Configuring the Snapshot Agent on Windows

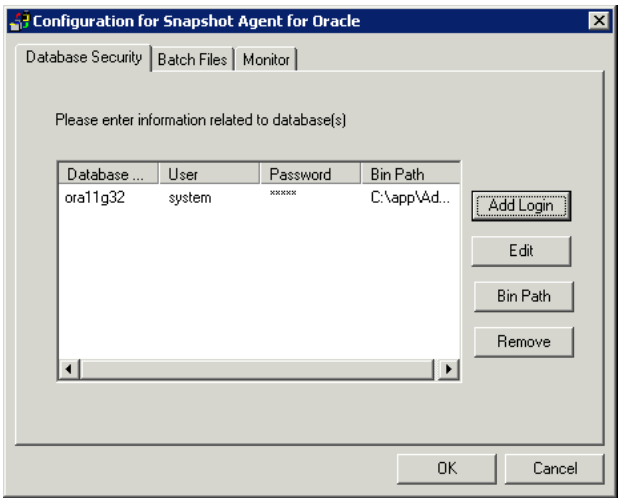
After the installation completes, a configuration utility runs. To run the utility manually, go to **Start** > **All Programs** > **SANClient** > **Snapshot Agent Configuration for Oracle**.

1. Select the version of Oracle you are using.



The Database security screen displays.

2. The Database Security tab displays a list of databases available for configuration.

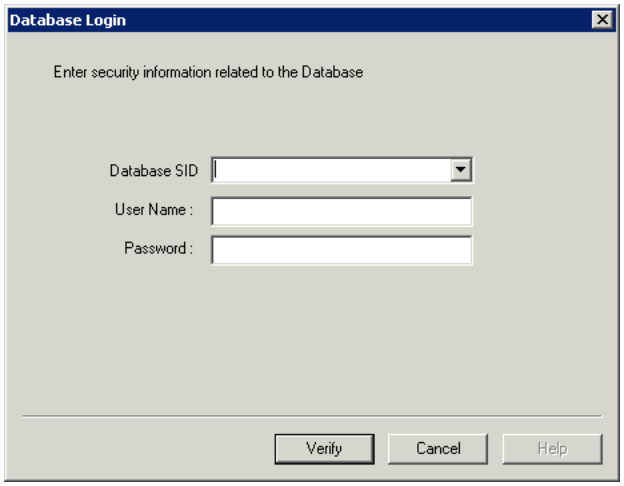


- **Add Login** – Enter the login credentials (database SID, User Name, and Password) for the database you are adding and then click the **Verify** button.
- **Edit** – The login credentials (database SID, User Name, and Password) for the selected database displays. Click the **Verify** button.
- **Bin Path** – Enter the Oracle bin path, typically **%ORACLE_HOME%/bin**. You can click the button next to the field to have the agent search for the path or you can manually enter the path.

  If you click the button and the SID is correct, the path is automatically discovered.

  If the SID is wrong, the path is not discovered. Either enter the correct SID or start the specified database, if it is not running.
- **Remove** – Click this button to remove the selected database from the list. To change the Database SID, User Name, or Password, click **Remove** to remove the existing SID and then re-add it.

3. Enter the database SID or select the database SID from the pull-down menu. Then enter the user name and password for the local computer and click the **Verify** button.



This is the system user and password that the storage server needs to access your database. When the Oracle database is set up initially, the default system user password is usually manager.

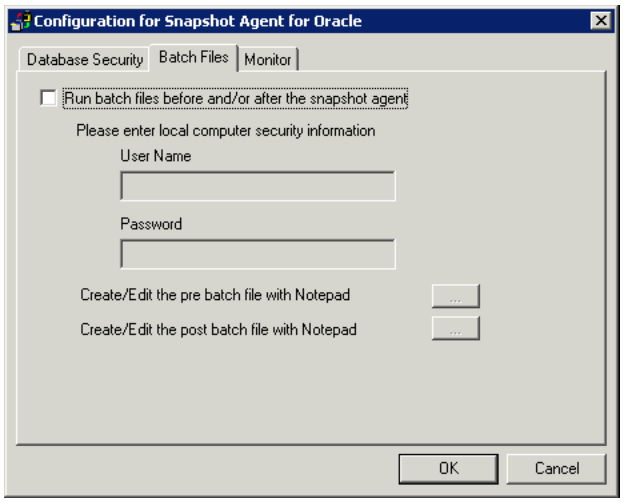
- **Database SID** – Enter the Oracle instance name.
- **User Name and Password** – Enter the user name and password of an Oracle account with DBA role. These are the user name and password that the storage server needs to access your database.

  When the Oracle database is set up initially, the default system user password is usually manager. Do not use *sys* for the user name.

Important

To change the Database SID, User Name, or Password, click the **Remove** button to remove the existing SID and then add it again.

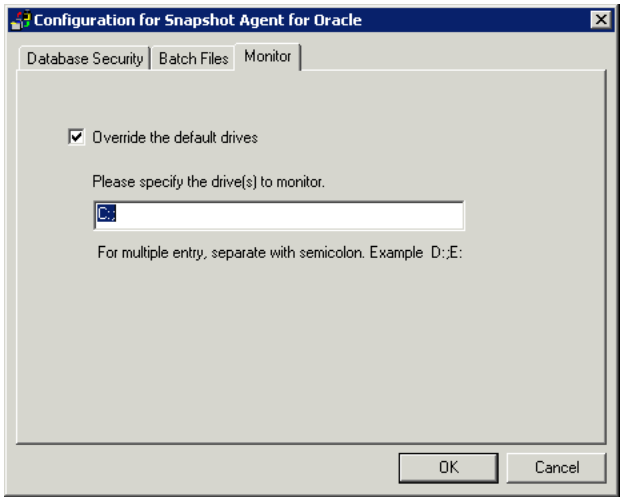
4. Click the **Verify** button so that the agent will verify the SID by connecting to the database with the provided information.
5. On the **Batch Files** tab, indicate if you want to run batch files before or after each snapshot.



To run batch files, you must enter an administrative user name and password for the local computer.

You can then click the **Create** and **Edit** buttons and use a text editor to generate the batch files.

6. On the **Monitor** tab, you can select to override the default drives and specify the drives on which you want the agent to look for databases.



Configuring ASM disks

The Snapshot Agent includes a utility that helps you configure Oracle Automatic Storage Management (ASM) disks.

asm10config -a | -d | -m | -l | -D

-a – add an ASM disk group

-d – delete an ASM disk group

-m – modify an ASM disk group

-l – list ASM disk groups

-D – delete all ASM disk groups

To add an ASM disk group:

1. Run the command

   /asm10config -a
2. Indicate if Oracle is started.
3. Enter the IP address of the storage server.
4. Enter the password for the root user on the storage server.
5. Enter the Oracle SID.
6. Set ORACLE_HOME.

   A list of virtual devices displays.
7. Select the virtual devices for your disk group by entering the appropriate line numbers.

   For multiple virtual devices, separate numbers with semicolons.

   For example: 1;2;5
8. If you have multiple disk groups, select the virtual device(s) for each.
9. Indicate if you want to save the displayed VGList information.

   The information is saved to **/usr/local/ipstorclient/agents/oracle10/etc/agt.ini**.

Configuring the Oracle Listener

The Snapshot Agent needs the Oracle Listener. Configure it to use:

- TCP/IP protocol
- Port number 1521

Each version of Oracle has its own Listener. If you have more than one version of Oracle running on the same machine, you must configure the Listener for all versions.

To configure the Oracle Listener:

1. Determine which version of Oracle was installed first.

For example, you have 9i and 10g installed on the same machine and 9i was installed first.

2. Run the Listener that came with the Oracle version you installed first.

   In this example, run the Listener that came with 9i.

3. Configure the other Oracle versions to use this Listener.

   In our example, configure the 10g version of Oracle to use the 9i Listener.

   See the Oracle documentation for information about configuring and using the Oracle Listener.

Installation on Linux

The following packages required for the configuration procedure:

- sanclient-4.50-0.965.i386.rpm
- oracle8i9i10g11agent-4.50-923.i386gen.rpm
- oracle-instantclient11.2-basic-11.2.0.1.0-1.i386.rpm

To install Snapshot Agent on a Linux system:

1. Install san client software and oracle instant client software.

   #rpm -ivh sanclient-4.50-0.965.i386.rpm
   #rpm -ivh oracle8i9i10g11agent-4.50-923.i386gen.rpm
   #rpm -ivh oracle-instantclient11.2-basic-11.2.0.1.0-1.i386.rpm

   Required for 64-bit systems only:

   #rpm -ivh oracle-instantclient11.2-basic-11.2.0.1.0-1.i386.rpm

2. Re-login and start san client.

   #su - root

   #sanclient start

3. Add server by command "sanclient monitor".

   #sanclient monitor

4. Send target to Promise server by command "iscsiadm".

   #iscsiadm -m discovery -t st -p <promiseserverip>:3260

5. Create iSCSI target manually on Promise VTrak S3000 management console and assign disk to the client.

6. Add the IP address of Client hosting Oracle DB and the Agent.

   In the VTrak S3000 console, expand SAN Client, right click the <Client Name> and select **Properties** > **Add IP address of SAN Client** and click the **OK** button.

7. Restart iscsi service.

   #service iscsi restart

8. Restart san client service.

   #sanclient restart

9. Use sanclient monitor to check the device status.

   # sanclient monitor

   Make sure the highlight Device is detected.

   SAN Client v4.50 (Build 965)
   Copyright 2001-2005 by FalconStor. All Rights Reserved.

   Select an item:
   0. < Quit >
   1. List SAN Client Configuration
   2. List SAN Devices
   3. Add Storage Servers
   4. Delete Storage Servers
   5. Rescan SAN Devices
   6. Attach SAN Devices
   7. Detach SAN Devices
   8. Enable Protocol
   9. Disable Protocol
   10. View Configured Protocol

   Choose option: 2

iSCSI Devices:

/dev/sdb: HBA 3 channel 0 target 0 lun 0

10. Install Oracle Agent for Linux package.

    # rpm -ivh oracle8i9i10g11agent-4.50-0.923.i386gen.rpm --nodeps

    Preparing... ### [100%]

    1:sanora ### [100%]

    Snapshot Agent for Oracle installation completed.

11. Append the following statement in **/etc/profile** or **/etc/csh.login**.

    LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<OraLibPath>; export LD_LIBRARY_PATH #ISORAENV

    where **<OraLibPath>** is the Oracle library path.

12. Shut down the client and then log out.
13. Then log in again as **root** and run the command

    /usr/local/sanclient/agents/oracle/bin/ora_setup.sh

    to configure this Snapshot Agent for Oracle.

14. Stop the SAN client and log in again as **root**.

    # sanclient stop

    SAN Client v4.50 (Build 965)

    Copyright 2001-2005 by FalconStor. All Rights Reserved.

    Stopping SANClient Client SNMP [OK]

    Stopping SANClient Client Daemon [OK]

    # su - root

Configuring the Snapshot Agent on Linux

To configure Snapshot Agent on a Linux system:

1. Configure Oracle agent setup.

   # /usr/local/sanclient/agents/oracle/bin/ora_setup.sh

   Oracle Agent Setup

   Enter 1 for Oracle 8 agent setup

   Enter 2 for Oracle 9 agent setup

   Enter 3 for Oracle 10 agent setup

   Enter 4 for Oracle 11 agent setup

   Which Oracle agent would you like to setup? 4

   Snapshot agent for Oracle 11 setup

   What is the Oracle lib32 path for shared library libclntsh.so.11.1

   /usr/lib/oracle/11.2/client/lib/

2. Make sure the Oracle lib32 path

   /usr/lib/oracle/11.2/client/lib/ for shared library libclntsh.so.11.1

   is added to

   LD_LIBRARY_PATH or LIBPATH

   Example: **export LD_LIBRARY_PATH=ORACLE_HOME/lib32:LD_LIBRARY_PATH**

   The following is the current LD_LIBRARY_PATH:

   /usr/local/sanclient/lib:/usr/local/sanclient/lib:/home/oracle/app/oracle/product/11.2.0/db_1/lib:/usr/lib/oracle/11.2/client/lib/

3. Make sure the above environment setting is in the profile.

   Would you like to continue the setup for Oracle agent? (y/n) y

   Snapshot Agent Setup for Oracle 11

   If there are more than one Oracle SID, please make sure all the Oracle SID instances are running.

4. Answer the following questions to configure the Snapshot Agent.
   Make sure Oracle instance test is running.

   Is Oracle started? (y/n) y

   What is the Oracle SID? test

   What is the Oracle home path for SID test? /home/oracle/app/oracle/product/11.2.0/db_1

   What is the Oracle admin user id for SID test? (system)

   What is the Oracle admin password for SID test? (manager)

   What is the login name of the UNIX user account that owns Oracle software? oracle

   Would you like to enter another Oracle SID? (y/n) n

   Snapshot Agent for Oracle has been set up successfully
5. Log in again and make sure the
   - SANClient is running
   - SANClient can communicate with the Promise VTrak S3000 server
6. Log in again and restart SAN client.

   # su - root

   # sanclient restart
7. Take a snapshot and verify the system log.

Turning On Oracle Archive Logging

You must turn on Oracle Archive Logging before running the Snapshot Agent.

To turn on Oracle Archive Logging:

1. Include the following three lines in your **initSID.ora**:

   log_archive_start = true

   log_archive_dest   = /mount_point/oradata/SID/ARCHIVE/

   log_archive_format = _%s.arc

   - l**og_archive_start** – This parameter specifies whether archiving should be started automatically when the database is started.
   - **log_archive_dest** – This value specifies the default location of the file to be used when archiving redo log files.
   - **log_archive_format** – This parameter is used to specify the default file name format for the archive log files. This value is appended to the **log_archive_dest value** (%s is the log sequence number).

   Therefore, when a redo log is archived, Oracle will use a combination of **log_archive_dest** and **log_archive_format** to produce the location and file name of the archive log. For example,

   /mount_point/oradata/SID/ARCHIVE/arch_1234.arc
2. Before restarting the database, verify that you have created the **/mount_point/oradata/SID/ARCHIVE** directory.

   Note that the trailing arc in **log_archive_dest** is part of the archive log file name, not the directory.

   These changes do not take effect until you restart the database.
3. With the database shut down, use one of the many DBA tools available, such as **sqlplus**, to manually start the database and execute the following commands:

   startup mount exclusive pfile=<path to pfile>

   connect internal

   alter database archivelog;

   archive log start;

   alter database open;

Running the Snapshot Agent

The Snapshot Agent triggers automatically any time a snapshot operation occurs on the Oracle drive.

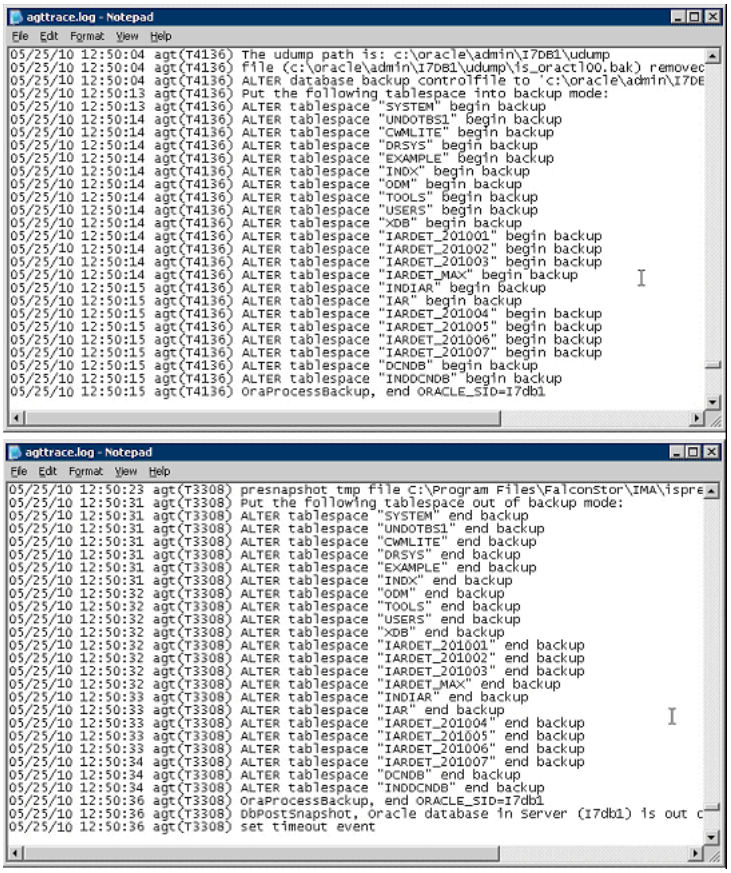
To test the Snapshot Agent, you can perform a Snapshot Copy of a virtual drive from the Console.

Important

Use a group if your Oracle database uses multiple virtual devices.

Confirming Snapshot Status

You can get detailed information from the agent trace log. You can find agttrace.log under the IMA installation folder. It is usually installed in **C:\Program Files\IMA**. There, you can see the connection to Oracle system and the ALTER tablespace begin backup and ALTER tablespace end backup command to all tablespaces on the protected disk.


agttrace.log - Notepad
File Edit Format View Help
05/25/10 12:50:04 agt(T4136) The udump path is: c:\oracle\admin\I7DB1\udump
05/25/10 12:50:04 agt(T4136) file (c:\oracle\admin\I7DB1\udump\is_oractl00.bak) removec
05/25/10 12:50:04 agt(T4136) ALTER database backup controlfile to 'c:\oracle\admin\I7DE
05/25/10 12:50:13 agt(T4136) Put the following tablespace into backup mode:
05/25/10 12:50:13 agt(T4136) ALTER tablespace "SYSTEM" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "UNDOTBS1" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "CWMLITE" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "DRSYS" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "EXAMPLE" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "INDX" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "ODM" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "TOOLS" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "USERS" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "XDB" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "IARDET_201001" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "IARDET_201002" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "IARDET_201003" begin backup
05/25/10 12:50:14 agt(T4136) ALTER tablespace "IARDET_MAX" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "INDIAR" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "IAR" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "IARDET_201004" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "IARDET_201005" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "IARDET_201006" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "IARDET_201007" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "DCNDB" begin backup
05/25/10 12:50:15 agt(T4136) ALTER tablespace "INDDCNDB" begin backup
05/25/10 12:50:15 agt(T4136) OraProcessBackup, end ORACLE_SID=I7db1
agttrace.log - Notepad
File Edit Format View Help
05/25/10 12:50:23 agt(T3308) presnapshot tmp file C:\Program Files\FalconStor\IMA\ispre
05/25/10 12:50:31 agt(T3308) Put the following tablespace out of backup mode:
05/25/10 12:50:31 agt(T3308) ALTER tablespace "SYSTEM" end backup
05/25/10 12:50:31 agt(T3308) ALTER tablespace "UNDOTBS1" end backup
05/25/10 12:50:31 agt(T3308) ALTER tablespace "CWMLITE" end backup
05/25/10 12:50:31 agt(T3308) ALTER tablespace "DRSYS" end backup
05/25/10 12:50:31 agt(T3308) ALTER tablespace "EXAMPLE" end backup
05/25/10 12:50:31 agt(T3308) ALTER tablespace "INDX" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "ODM" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "TOOLS" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "USERS" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "XDB" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "IARDET_201001" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "IARDET_201002" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "IARDET_201003" end backup
05/25/10 12:50:32 agt(T3308) ALTER tablespace "IARDET_MAX" end backup
05/25/10 12:50:33 agt(T3308) ALTER tablespace "INDIAR" end backup
05/25/10 12:50:33 agt(T3308) ALTER tablespace "IAR" end backup
05/25/10 12:50:33 agt(T3308) ALTER tablespace "IARDET_201004" end backup
05/25/10 12:50:33 agt(T3308) ALTER tablespace "IARDET_201005" end backup
05/25/10 12:50:33 agt(T3308) ALTER tablespace "IARDET_201006" end backup
05/25/10 12:50:34 agt(T3308) ALTER tablespace "IARDET_201007" end backup
05/25/10 12:50:34 agt(T3308) ALTER tablespace "DCNDB" end backup
05/25/10 12:50:34 agt(T3308) ALTER tablespace "INDDCNDB" end backup
05/25/10 12:50:36 agt(T3308) OraProcessBackup, end ORACLE_SID=I7db1
05/25/10 12:50:36 agt(T3308) DbPostSnapshot, Oracle database in Server (I7db1) is out c
05/25/10 12:50:36 agt(T3308) set timeout event

Removing Snapshot Agent

Windows

To uninstall the Snapshot Agent software from a Windows system:

Use **Add/Remove Programs** from the Control Panel .Linux

To uninstall the Snapshot Agent software from a Linux system:

1. Log onto the system as root.
2. Run the command,

   rpm -e oracleniagent-<version number>-<build number>

   rpm -e oracle8i9i10g11agent-4.50-923.i386gen.rpm

Protecting and Recovering Oracle Databases

Database Design with Virtual Devices

Physical location of the tablespaces

We recommend that you create each tablespace on a separate virtual disk. If there are sufficient resources, the virtual disk should be created on a dedicated physical device. It this is not possible, the virtual disks should be created such that disk access is balanced across the available physical resources.

Fault tolerance and performance considerations

For fault tolerance, mirroring can be done at the operating system level or you can use the Mirroring feature. Other fault tolerance configurations can be implemented at the operating system level. When creating virtual devices, keep in mind that the operating system might configure the virtual disks in a RAID configuration. For RAID configurations, you should make sure the disks are from different physical disks.

Free disk space considerations

If the database is very active and changes are made randomly, the Snapshot Resource should be created with sufficient size, and the storage server should have enough free disk space to allow the snapshot resource to grow when needed. It is better to define which physical disk it should use when expanding the snapshot resource.

Using groups

Most Oracle databases use more than one virtual disk. In order to guarantee database integrity, you should use the Group feature.

To configure a group:

1. Create a group with Snapshot enabled.
2. Select the virtual disks that are used by the Oracle database to join the group.
3. Assign the group to the client that runs the Oracle database.
4. Perform all snapshot related functions using the group.

Data Backup and Protection Scenarios

Snapshot

The Snapshot option is an effective way to protect your Oracle database by creating point-in-time snapshot copies of the database. You can use these Snapshots to recover your database back to the time when the Snapshot was triggered.

To create a Snapshot:

1. Connect to the server that is serving the virtual disks for the Oracle database.
2. In the Tree, expand **Logical Resources** > **Groups**.
3. Right-click the group that was created for the Oracle database and select **Snapshot** > **Create**.
4. Enter a descriptive name for the Snapshot.
5. Ensure that the Snapshot Agent has completed taking a snapshot of the disks.

   The Database Alert log should display messages showing that all tablespaces have been in and out of the backup mode.
6. In the Tree, expand the group and select one of the virtual disks.
7. On the right pane for the virtual disk, click the **Snapshot** tab.

   A list of Snapshots appears, with the most recent Snapshot listed at the end.

Snapshot Copy

You can use Snapshot Copy to create a physical copy of the disks used by the Oracle database. The set of Snapshot Copy disks should be created with the same Snapshot. The set of Snapshot Copy disks are exactly what the online Oracle disks looked like at the moment you created the Snapshot.

This set of disks can be mounted on the Oracle Server and the Oracle database instance can be started with minimal recovery steps. Make sure there is enough free physical space for creating the Snapshot Copy.

To create a Snapshot Copy:

1. Launch the Management Console.
2. Connect to the server that is serving the virtual disks for the Oracle database.
3. In the Tree, expand **Logical Resources** > **SAN Resources**.
4. Right-click the first virtual device of the group.
5. Select **Snapshot** > **Copy**.
6. Select the desired Snapshot to be copied.
7. Repeat the last two steps for all virtual devices in the group.

The Snapshot Copy disks can be assigned and mounted by the client using the Oracle database. When you start the Oracle database using the Snapshot Copy disks, the tablespaces are still in backup mode. Refer to the Disk failure section for information about how to recover a database with Snapshot Copy disks.

SnapshotView

Instead of recreating the Oracle disks with physical storage, you can create a SnapshotView that is mountable and works exactly like the Snapshot, except that the original set of disks for the production database have to be working. You can use SnapshotView to retrieve lost data without rolling back changes on the product database. SnapshotView does not require physical storage.

To create a SnapshotView of the database disks:

1. Launch the Management Console.
2. Connect to the server that is serving the virtual disks for the Oracle database.
3. In the Tree, expand **Logical Resources** > **SAN Resources**.
4. Right-click the first virtual device of the group.
5. Select Snapshot > SnapshotView.
6. Select the desired Snapshot to be viewed.
7. Repeat the last two steps for all virtual devices in the group.

You will see a new virtual disk for the SnapshotView you created for each disk in the group. You can assign SnapshotView virtual disks to a client and mount them just as you can any other virtual disks. You can copy files from the SnapshotView disks. You can start the Oracle database on the SnapshotView disks and export tables from that instance of the Oracle database. The tablespaces are set to backup mode when the snapshot occurs.

When you first start your database using the SnapshotView disks you must recover the database to set the tablespaces back to normal mode.

Replication

You can set up replication of the Oracle database disks to protect the database in case of site failure. If the primary site fails, the replica disks on the secondary site can be promoted, assigned to the Oracle server, and mounted. As a result, the database is up and running with minimal down time. The database reflects the state of the last complete replication.

Snapshot Rollback

Another useful feature is the rollback of a Snapshot. The disk can be roll back to the point in time when you took the Snapshot. It is useful for rolling back changes to a known good stage, such as before a major update to a table that contains customer information.

To perform a Snapshot rollback:

1. Stop the Oracle database.
2. Stop the client on the Oracle database server.
3. Launch the Console.
4. From the SAN client or IMA, unassign the devices that the Oracle database resides on.
5. Connect to the server that is serving the virtual disks for the Oracle database.
6. In the Tree, expand **Logical Resources** > **Groups**.
7. Right-click the group that was created for the Oracle database.
8. Select **Snapshot** > **Rollback**.
9. Select the Snapshot that you want to roll back to.
10. Follow the wizard to complete the rollback procedure.
11. Start the client on the Oracle database server.
12. Start the Oracle database.
13. From the SAN client or IMA, reassign the devices that the Oracle database resides on.
14. Perform the Database recovery, if necessary, by typing recover database in SQL Plus or a command window.

Complete backup using a SnapshotView or Snapshot Copy

You can perform a complete tape backup of your database using a SnapshotView or Snapshot Copy. The SnapshotView or Snapshot Copy disks contain the Oracle database files as regular files and can be backed up with your normal backup software.

Recovery Scenarios

Disk Failure

You can quickly recover from disk failure by using a Snapshot Copy you created. The database can be brought back online in a matter of minutes. However, the data entered after the Snapshot was created cannot be restored.

To recover using a Snapshot Copy:

1. Stop the client on the Oracle database.
2. Launch the Management Console.
3. Unassign all of the disks used for the Oracle database from the client.
4. Assign the set of Snapshot Copy disks for the Oracle database to the client.
5. Restart the client on the Oracle database server.
6. Start the Oracle database.
7. Recover the database, if necessary.
8. Open the database for normal access.

User Failure

User failure can occur when users executes DDL commands, such as drop table. The Snapshot option and the Snapshot Agent can recover tables and records that were accidentally dropped.

To recover from user failure:

1. Create a SnapshotView of the database disk using the desired Snapshot.
2. Assign the SnapshotView virtual disks to a backup Oracle database server. This could be the on same server as the production database server.
3. Rescan the client to discover the disks.
4. Start the Oracle database instance using the SnapshotView disks.
5. Export the object (such as a table) from this database instance to a dump file.
6. On the production database, drop the object that was altered by the user.
7. Import the object to the production database using the dump file.

Operator failure

If the system administrator or DBA accidentally deleted some files that are important to the Oracle database, you can quickly retrieve the files from a SnapshotView.

To recover files from a SnapshotView:

1. Create a SnapshotView of the database disk using the desired Snapshot.
2. Assign the SnapshotView virtual disks to the Oracle database server.
3. Rescan the client to discover the new disks.
4. Mount the new disks and copy the files from the SnapshotView disks.

If a disk for the database is accidentally formatted, you can recover it using rollback. See “Snapshot Rollback” on page 17 for more information.

Restoring Backed-up Oracle Databases

The backed up version of an Oracle database cannot be mounted until an Oracle **end backup** command is issued.

If you issue the **startup open pfile=...** command without the **end backup** command being issued, you get a message telling you that the database *needs media recovery*. For example:

```
SQL> connect sys/password as sysdba
Connected to an idle instance.
SQL> startup open pfile=/oracle/pfile/init.ora
ORACLE instance started.
Total System Global Area  403473660 bytes
Fixed Size                  279804 bytes
Variable Size            201326592 bytes
Database Buffers         201326592 bytes
Redo Buffers                540672 bytes
Database mounted.
```

ORA-01113: file 1 needs media recovery

ORA-01110: data file 1: '/oracle/system/SYSTEM.dbf'

Note that it says *file 1* needs recovery. While there may be multiple files, the **startup** stops after seeing the first error and does not try to continue to the other data files.

Automatic recovery

1. When you see this message, you can run the **recover database** command to find all tablespaces and take each out of backup mode.

   SQL> **recover database;**

   Media recovery complete.

2. Afterwards, you can open the database.

   SQL> **alter database open;**

   Database altered.

Manual recovery

You can also manually issue the Oracle commands to find each tablespace and then end the backup:

1. Instead of issuing the “recover database” command, check to see if the tablespaces are in the “backup mode” by issuing the following command.

   SQL> **select * from v$backup;**

FILE#	STATUS	CHANGE#	TIME
1	ACTIVE	107569	23-AUG-00
2	ACTIVE	107573	23-AUG-00
3	ACTIVE	107577	23-AUG-00
4	ACTIVE	107581	23-AUG-00
5	ACTIVE	107585	23-AUG-00
6	ACTIVE	107589	23-AUG-00

   6 rows selected.

Since the file status is active, the tablespaces are still in the backup mode.

2. Find out what the names of the tablespaces are.

   SQL> **select * from v$tablespace**;

TS#	NAME	INC
0	SYSTEM	YES
1	UNDOTBS	YES
2	DRSYS	YES
3	INDX	YES
4	TEMP	YES
5	TOOLS	YES
6	USERS	YES

   7 rows selected.

3. Manually take each out of backup mode.

   SQL> **ALTER TABLESPACE SYSTEM END BACKUP;**

   Tablespace altered.

   SQL> **ALTER TABLESPACE UNDOTBS END BACKUP;**

   Tablespace altered.

   SQL> **ALTER TABLESPACE DRSYS END BACKUP;**

   Tablespace altered.

   SQL> **ALTER TABLESPACE INDX END BACKUP**;

Tablespace altered.

SQL> **ALTER TABLESPACE TOOLS END BACKUP**;

Tablespace altered.

SQL> **ALTER TABLESPACE USERS END BACKUP;**

Tablespace altered.

4. Open the database.

   SQL> **ALTER DATABASE open;**

   Database altered.

Chapter 4: Snapshot Agent for Microsoft® SQL Server

- Supported Versions (page 21)
- Installation (page 21)
- Configuring the Snapshot Agent (page 22)
- Advanced Configuration (page 25)
- Run the Snapshot Agent (page 27)
- Confirm Snapshot Status (page 27)
- Remove Snapshot Agent Software (page 28)

The Snapshot Agent for Microsoft SQL Server protects Microsoft SQL Server databases with full point-in-time consistency while still allowing full speed, non-stop access to the databases.

Prior to starting the snapshot process, a request is sent to the application server running the Snapshot Agent for Microsoft SQL Server. For databases with the Recovery Model set to **Simple** or **Full**, the Snapshot Agent performs a full SQL Backup Database Snapshot.

Using backup software, a back up of the snapshot image can be performed at high speed while Microsoft SQL Server operates in normal mode. Because the contents of the snapshot image are guaranteed never to change, what is backed up is consistent, ensuring transactional integrity. While the backup software is reading data from the snapshot image, changes that occur to the database will not affect what gets written. Users are always able to see the database with full access at all times while the backup software sees a stable, read-only snapshot image of the database taken an instant before the backup began.

Supported Versions

The Snapshot Agent for Microsoft SQL Server is supported for Windows Enterprise Server platforms. For specific version information, refer to the Certification Matrix on the www.promise.com website.

Installation

Installation of the Snapshot Agent has the following requirements:

- Before you install the Snapshot Agent, you must install PROMISE SAN Disk Manager (SDM/IMA) on the same machine.

  If SDM/IMA is not detected when Snapshot Agent installation begins, an error message displays. Cancel the procedure, install SDM/IMA, and then repeat Snapshot Agent installation.
- The Snapshot Agent has to be installed on the same machine where the SQL Server database is running.
- Your SQL Server must be started before installing the agent.
- You must be an administrator or have administrator privileges in order to install the Snapshot Agent.

To install:

1. Launch installation from the installation media.
2. When prompted, enter your license key code.

   The Snapshot Agent license must be registered with PROMISE.
   - If your computer has an Internet connection, the license is activated as soon as you enter your key code and click the **Next** button.
   - If your Internet connection is temporarily down, your license activates automatically the next time the Snapshot Agent is started and your Internet connection is working.
   - If your computer has no Internet connection, you must perform an offline activation. See the *VTrak S3000 Quick Start Guide* for more information.

   You have 30 days to activate your license so that you can continue to use the Agent.
3. When done, click **Finish**.

   The Agent installs to the same directory as SDM/IMA.

Silent installation

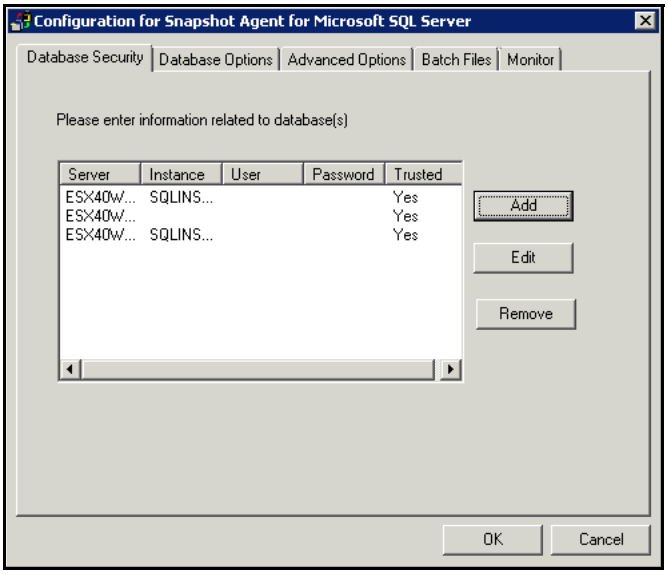
The Snapshot Agent provides the ability to perform a silent install. A silent install does not require any interaction during the installation process.

In order to install the Snapshot Agent in silent mode, run **setup /s** or **setupsilent.bat**.

Configuring the Snapshot Agent

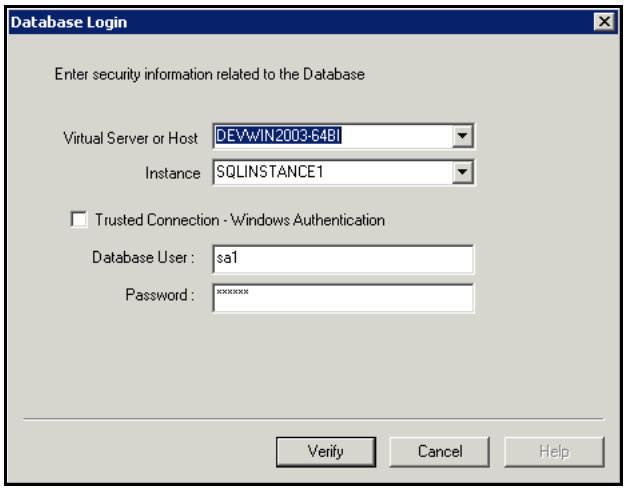
After the installation completes, a configuration utility launches. To access this utility at a later time, choose **Start** > **All Programs** > **SANClient** > **Configuration for Snapshot Agent for Microsoft SQL Server**.

1. On the **Database Security** tab, register each SQL instance.



The SQL Snapshot Agent supports multiple instances of Microsoft SQL on the same server. You have to register each instance name with the Snapshot Agent so that it can communicate with each instance.

Click the **Add** button to add another instance of Microsoft SQL on the server. The Database Login screen displays.



Choose the virtual server or host to which to add the instance. In addition, you can choose the **Trusted Connection – Windows Authentication** checkbox allowing you to avoid storing credentials in connection strings.

Virtual Server or Host – If the SQL server is in a cluster, select the name of the virtual server on which the SQL instance is created. If the server is not in a cluster, select the local host name. The drop down list displays the virtual server name and the host name that it detects from the registry.

Instance – Select the name of the SQL instance. For the default SQL instance, select **MSSQLSERVER**. You can use the **Services** console (**Control Panel** > **Administrative Tools** > **Services**) to check instance names. The instance name is listed in parentheses.

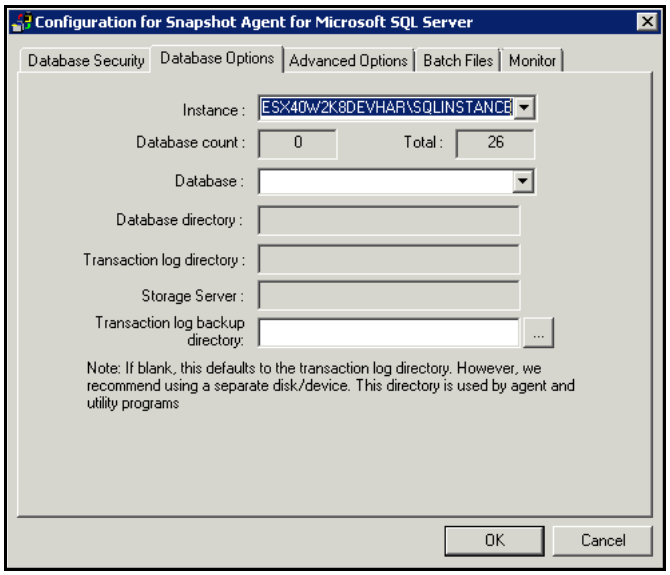
For example, if the service name is **SQL Server (MSSQLSERVER)**, its instance name is **MSSQLSERVER**. If you have another instance, you will see another service, such as **SQL Server (INSTANCE2)**. In this case, the SQL instance name is **INSTANCE2**.

Important

If you are using the default MSSQLSERVER instance with Trusted Windows Authentication, leave the default instance name blank.

User Name and Password – Enter the user name and password (Windows Authentication mode or SQL Server authentication mode) of the account that has access to the database.

2. On the **Database Options** tab, specify the location of the transaction log backup directory.

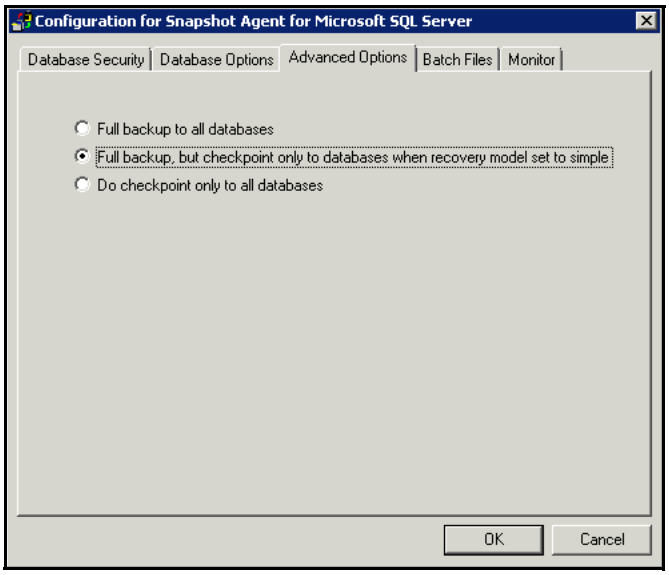


Database – Choose the database from the drop down list.

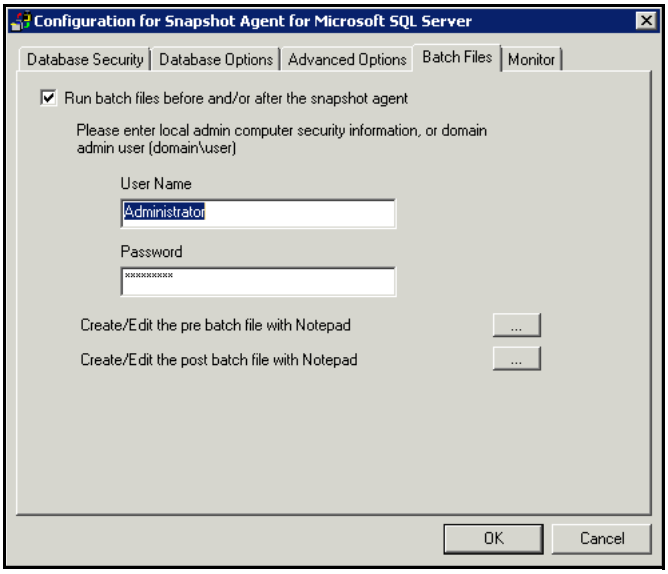
Transaction log backup directory – Specify the location. We recommend that the transaction log backups be on a disk separate from the transaction log and separate from the database.

3. On the **Advanced Options** tab, you can perform a:
   - **Full backup of all databases** – The default is to take a full backup of all databases
   - **Full backup but only do a checkpoint on databases** – Set the recovery model to **Simple**. For previous SQL Agent behavior

- **Checkpoint on all databases** – For a large number of databases.



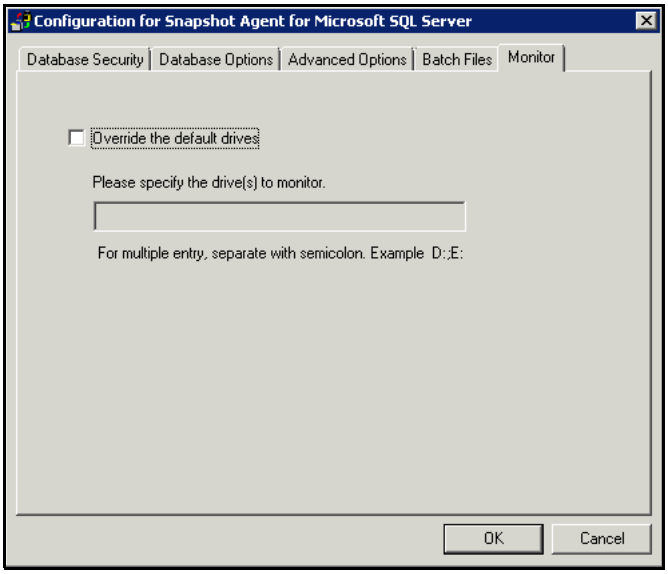
4. On the **Batch Files** tab, indicate if you want to run batch files before and/or after each snapshot.



In order to run batch files, you must enter an administrative user name and password for the local computer.

You can then click the **Create** and **Edit** buttons and use Notepad to generate the batch files.

5. On the *Monitor* tab, you can select to override the default drives and specify the drive(s) on which you want the agent to look for databases.



Advanced Configuration

Transaction Log Backups

A command line recovery tool **(fsssrest.exe** is included with your Snapshot Agent for Microsoft SQL installation, allowing you to perform additional transaction log backups after the full backup and before the last transaction log backup.

After a storage server snapshot, if needed, run this command to back up the transaction log:

fsssrest -d <databasename> -tlb

The advantage to using this command is that the date and time is recorded, making it easier to identify which transaction logs are needed during the restore. You can also schedule and perform Transaction Log backups with other utilities in order to have more transaction log backups between the snapshots (full backups).

You can run this command as needed, based on your backup schedule. The **<databasename>.his** file contains a list of all files from the time the application started and resides on the same disk as the specified transaction log disk.

The **<databasename>.his** file looks similar to the following:

dbtest.mdf

dbtest-20070212121500.log

dbtest-20070212123000.log

dbtest-20070212124500.log

dbtest.mdf

Command line utility

Usage: **fsssrest [action][options]**

actions

-fro <full restore only>
-tlb <transaction log backup>
-cp <checkpoint>
-list <list databases in instance>
-backuplist <list databases backedup in instance>

options

-t <trace path and file>
-d <databasename> | * (applies to tlb and cp)
-i <Server Name><Instance Name>
-en <english text>
-tlb Example usage on two instances:
fsssrest.exe -tlb -d "*" -i "ESX40W2K8DEVHAR\SQLINSTANCE1"
fsssrest.exe -tlb -d "*" -i "ESX40W2K8DEVHAR"

This command is recorded in the history files for SQL Recovery to use. Any Microsoft SQL recovery utility can use the transaction log backups.

Trace Log

To turn the Trace Log on and create a fstrace.log file, use the following command:

fsssrest -t

To create a fstrace.log file to another location or file name option (default):

fsssrest -t "d:\fstrace.log"

The Trace Log is also available from the console.

To create a **fstrace.log** file, select **Options** > **Trace**.

To view the Trace Log, select **View** > **Log**.

Run the Snapshot Agent

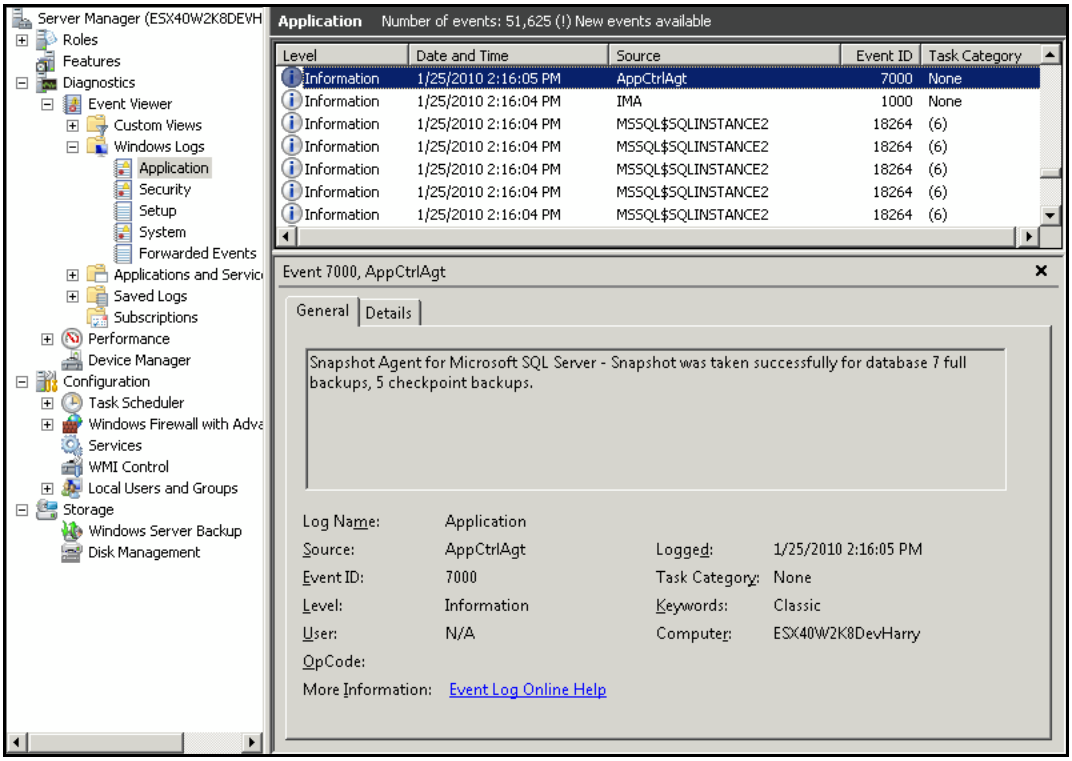
The Snapshot Agent triggers automatically any time a Snapshot operation occurs on the Microsoft SQL Server drive.

To test the Snapshot Agent, you can perform a Snapshot Copy of a virtual drive from the Console.

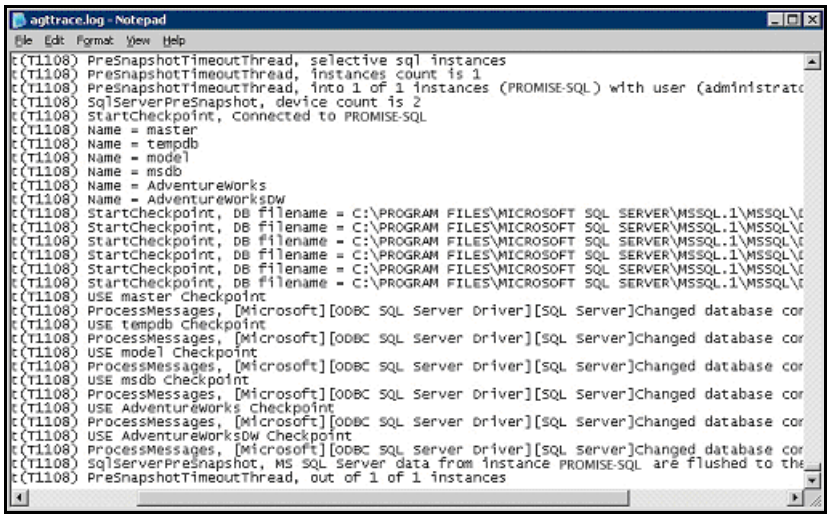
Confirm Snapshot Status

You can see numerous events from the SQL server in the Windows Event Log.

For example, you see an event similar to the picture below.



You can also get detailed information from the agent trace log. You can find **agttrace.log** under the IMA installation folder. It is usually installed in **C:\Program Files\IMA**. There, you can see the connection between the SQL instance and the SQL database list.



Remove Snapshot Agent Software

You can use **Add/Remove Programs** from the Control Panel.

Or navigate to the installation files on your installation media and follow the on-screen instructions to uninstall the Snapshot Agent.

Chapter 5: Snapshot Agent for MySQL

- Supported versions (page 29)
- Installation (page 29)
- Configuring the Snapshot Agent (page 29)
- Running the Snapshot Agent (page 29)
- Confirming Snapshot Status (page 29)
- Removing Snapshot Agent software (page 30)

PROMISE provides a Snapshot Agent for MySQL, a Relational Database Management System (RDBMS) in which data is stored in the form of tables and the relationship among the data is also stored in the form of tables. MySQL runs as a server providing multi-user access to a number of databases. MySQL is a key part of Linux, Apache, MySQL, PHP/Perl/Python (LAMP), an open source enterprise software stack. The MySQL Snapshot Agent ensures the MySQL database is in sync and stable before taking snapshots. It protects MySQL databases with full point-in-time consistency while still allowing full speed, non-stop access to the databases.

Supported versions

The Snapshot Agent for MySQL Server is supported for the Red Hat Enterprise Linux platform. For specific version information, refer to the Certification Matrix on the www.promise.com website.

Installation

Installation of the Snapshot Agent has the following requirements:

- Before you install the Snapshot Agent, you must install PROMISE SAN Disk Manager (SDM/IMA) on the same machine.

  If SDM/IMA is not detected when Snapshot Agent installation begins, an error message displays. Cancel the procedure, install SDM/IMA, and then repeat Snapshot Agent installation.
- The Snapshot Agent must be installed on the same machine where the MySQL database is running.
- The MySQL Server must be started before installing the agent.
- You must be an administrator or have administrator privileges in order to install the Snapshot Agent.

To install:

1. Launch installation from the installation media.
2. When prompted, enter your license key code.

   The Snapshot Agent license must be registered with PROMISE.
   - If your computer has an Internet connection, the license is activated as soon as you enter your key code and click the **Next** button.
   - If your Internet connection is temporarily down, your license activates automatically the next time the Snapshot Agent is started and your Internet connection is working.
   - If your computer has no Internet connection, you must perform an offline activation.

   You have 30 days to activate your license so that you can continue to use the Agent.

Configuring the Snapshot Agent

After the installation completes, you can set up the configuration by running the following:

/usr/local/ipstorclient/agents/mysql/bin/ismysql_setup

Running the Snapshot Agent

The Snapshot Agent triggers automatically any time a Snapshot operation occurs on the MySQL database files or drive.

Confirming Snapshot Status

You can also get detailed information from the agent trace log. You can find **agttrace.log** under the IMA installation folder. It is usually installed in **C:\Program Files\IMA**.

Removing Snapshot Agent software

You can uninstall the Snapshot Agent by typing the following:

rpm -e ismysql-4.50-0.906

Important

In this case the mysql agent is build **906** and the package name is **mysql-4.50-0.906.i386.rpm**. If you are using a different build, you must modify the command as appropriate.

Chapter 6: Snapshot Agent for VSS

- About Microsoft VSS (page 31)
- Snapshot Process (page 31)
- Supported Writers (page 32)
- Storage Configuration Guidelines (page 32)
- Installating the Snapshot Agent (page 32)
- Configuring the Snapshot Agent (page 33)
- Running the Snapshot Agent (page 35)
- Removing Snapshot Agent Software (page 35)

The PROMISE Snapshot Agent for Microsoft® Volume Shadow Copy Service (VSS) protects VSS-aware drives with full point-in-time consistency while still allowing non-stop access to the data.

About Microsoft VSS

Microsoft VSS provides the backup infrastructure for Microsoft Windows operating systems, using a set of extensible application programming interfaces (APIs) to create consistent point-in-time copies of data —shadow copies—across multiple volumes, regardless of the snapshot technology or application, by coordinating with business applications, file-system services, backup applications, fast recovery solutions, and storage hardware.

VSS consists of four components:

- **Requestors** – Start the VSS backup or restore operation and manage metadata.
- **Writers** – Prepare applications for backups and restores.
- **Hardware Providers** – Create the snapshot shadow copies by communicating with hardware.
- **VSS Service** – Windows service that controls VSS operations by coordinating the other components.

Snapshot Agent for VSS

The PROMISE Snapshot Agent for VSS takes consistent point-in-time snapshots of VSS-aware application data and coordinates snapshot creation with VTrak S3000 server.

The PROMISE Snapshot Agent for VSS has its own requestor and hardware provider. The hardware provider is compatible with any third-party requestor.

Supported Versions

The Snapshot Agent for VSS is supported on the Windows Enterprise Server platforms. For specific version information, refer to the Certification Matrix on the www.promise.com website.

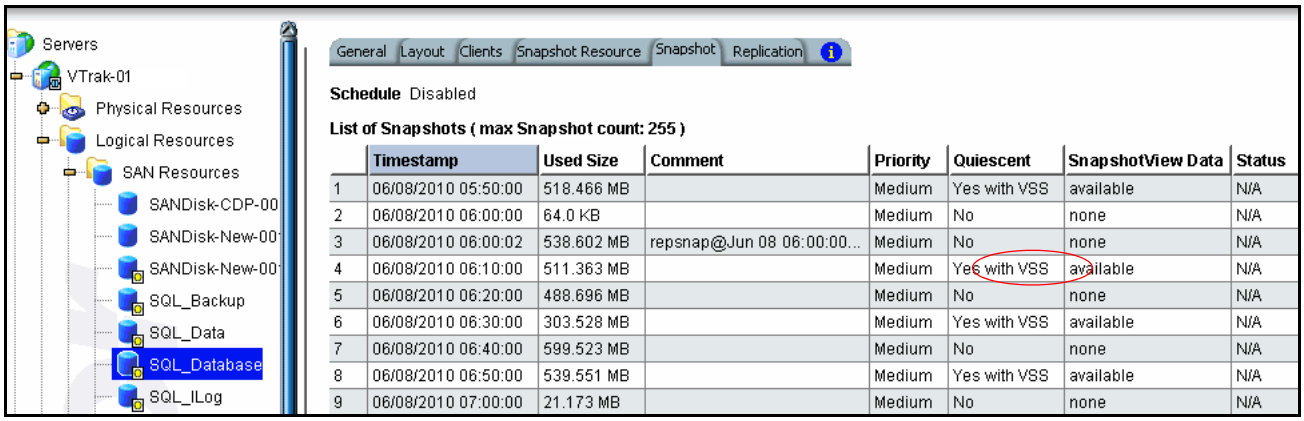
Snapshot Process

The difference between the normal snapshot process and the process used by the Snapshot Agent for VSS is that the SnapshotView is assigned after the snapshot is created. The requestor for the Snapshot Agent clears read-only and hidden flags and saves writer metadata to each volume. The hardware provider performs additional cleanup and then tells VTrak S3000 server to unassign and delete the SnapshotView; SnapshotView data is saved.

When you select a SAN Resource in the PROMISE Management Console, Snapshots created using the Snapshot Agent for VSS show **Yes with VSS** in the Quiescent column.

SnapshotView Data values can be:

- **Available** – SnapshotView data is present
- **None** – There is no SnapshotView data
- **In use** – SnapshotView is active



	Timestamp	Used Size	Comment	Priority	Quiescent	SnapshotView Data	Status
1	06/08/2010 05:50:00	518.466 MB		Medium	Yes with VSS	available	N/A
2	06/08/2010 06:00:00	64.0 KB		Medium	No	none	N/A
3	06/08/2010 06:00:02	538.602 MB	repsnap@Jun 08 06:00:00...	Medium	No	none	N/A
4	06/08/2010 06:10:00	511.363 MB		Medium	Yes with VSS	available	N/A
5	06/08/2010 06:20:00	488.696 MB		Medium	No	none	N/A
6	06/08/2010 06:30:00	303.528 MB		Medium	Yes with VSS	available	N/A
7	06/08/2010 06:40:00	599.523 MB		Medium	No	none	N/A
8	06/08/2010 06:50:00	539.551 MB		Medium	Yes with VSS	available	N/A
9	06/08/2010 07:00:00	21.173 MB		Medium	No	none	N/A

Supported Writers

The Snapshot Agent for VSS is designed to make backups uniform across applications. However, each writer has distinct behaviors, the most important of which are noted below.

Microsoft® Exchange 2010/Exchange 2007

For snapshots of Exchange databases and log files on shadow copy devices, the agent can verify the checksum of the database and log files on the SnapshotView. Snapshot verification may take a long time to complete, and can be disabled in the agent configuration tool. See “Configuring the Snapshot Agent” on page 33.

Microsoft® SQL 2008

Supported.

Microsoft® Hyper-V

In order for a virtual machine to take part in the VSS process, it must have the Hyper-V integration tools installed; otherwise, the virtual machine is temporarily suspended and saved to the disk during snapshot creation. When the SnapshotView devices are assigned to the host during a full backup, the Hyper-V writer will rollback each virtual machine to the same consistent point-in-time.

Microsoft® Active Directory 2008/Microsoft® Active Directory 2008 R2

Supported.

Storage Configuration Guidelines

- Microsoft VSS requires that devices are formatted in NTFS.
- Microsoft VSS limits the number of volumes in a group to 64.
- All devices in a snapshot group must be assigned to the client.
- *Snapshot* needs to be enabled on both Primary and Replica disk.
- If *Continuous Replication* is enabled on a device, then select the Snapshot options *Create Primary Snapshot* and *Synchronize Replica Snapshot*.
- Dynamic disks are not supported.

Installating the Snapshot Agent

Installation of the Snapshot Agent for VSS has the following requirements:

- Before you install the Snapshot Agent, you must install PROMISE SAN Disk Manager (SDM/IMA) on the same machine.

  If SDM/IMA is not detected when Snapshot Agent installation begins, an error message displays. Cancel the procedure, install SDM/IMA, and then repeat Snapshot Agent installation.
- The agent can be installed on any client that supports Microsoft VSS.
- You must be an administrator or have administrator privileges in order to install the Snapshot Agent.

To install the Snapshot Agent:

1. Launch installation from the installation media.
2. When prompted, enter your license key code.

   The Snapshot Agent license must be registered with PROMISE.

   - If your computer has an Internet connection, the license is activated as soon as you enter your key code and click the **Next** button.
   - If your Internet connection is temporarily down, your license activates automatically the next time the Snapshot Agent is started and your Internet connection is working.
   - If your computer has no Internet connection, you must perform an offline activation.

   You have 30 days to activate your license so that you can continue to use the Agent.
3. When done, click **Finish**.

   The Snapshot Agent for VSS installs to the same directory as SDM/IMA.

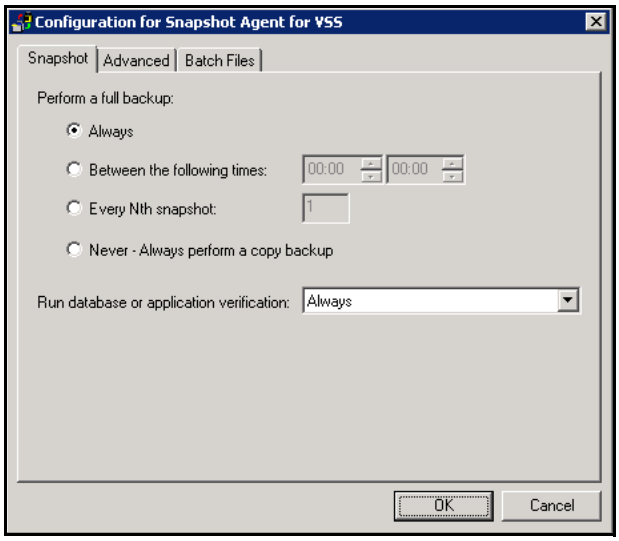
Silent Install

The Snapshot Agent provides the ability to perform a silent install, which requires no user interaction during the installation process.

In order to install the Snapshot Agent in silent mode, run **setup /s** or **setupsilent.bat**.

Configuring the Snapshot Agent

After the installation completes, a configuration utility launches. To access this utility at a later time, choose **Start** > **All Programs** > **SANClient** > **Configuration for Snapshot Agent for VSS**, which runs **vsscfg.exe**.



Performing a Full Backup

The **Snapshot** tab allows you to configure or disable full backups and copy backups. Each writer decides now to handle a copy backup, but typically, log files are not truncated.

- **Always** – The default. Always perform a full backup.
- **Between the following times** – If a Snapshot notification occurs between the times you specify, the Snapshot is a full backup.
- **Every Nth snapshot** – Snapshots are counted, with the first Snapshot following a full backup designated as 1. When the count reaches the number you specify, that Snapshot is a full backup. For example, if you set the value to 5, every fifth Snapshot is a full backup.

  Note that if you change this value to a lower number and the count is currently higher, the next backup is a full backup. Then the count restarts.
- **Never** – Always perform a copy backup.

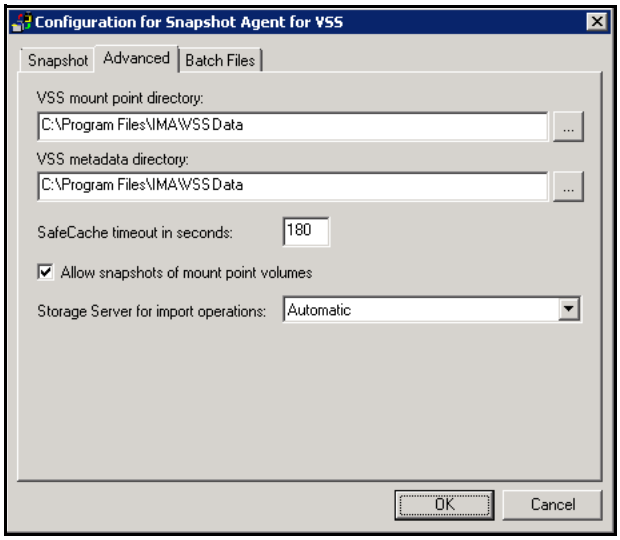
Running Database or Application Verification

You can specify when the SnapshotView should be verified during the snapshot process. Currently, verification is compatible only with Microsoft Exchange, and checks to see if Exchange is involved after snapshot creation is finished. You can disable this option if the process takes too much time. For Exchange snapshots, the agent will verify the checksum of the database and log files on the SnapshotView, similar to IntegrityTrac.

- **Always** – Always run the verification.
- **After a full backup –** The default. Run the verification if the current snapshot is a full backup.
- **Never** – Never run the verification.

Advanced Options

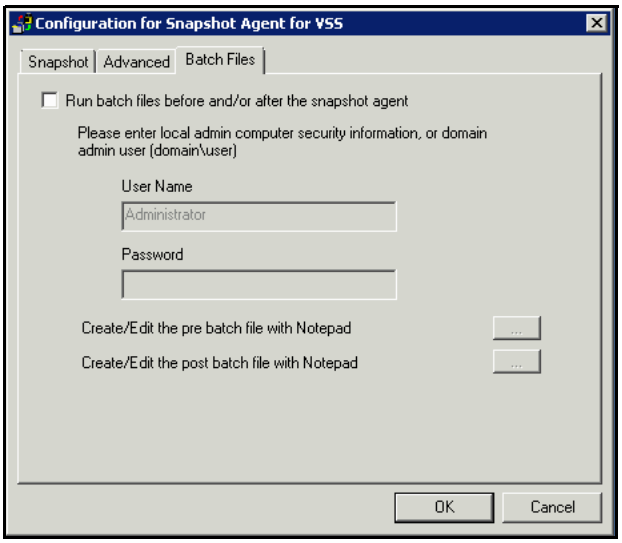
Use the advanced options to further refine snapshot configuration.



- **VSS mount point directory** – The directory on which SnapshotView volumes are mounted. Drive letters are not assigned to the SnapshotView volumes.
- **VSS metadata directory** – The directory where requestor and writer metadata is stored. You can also specify a file share in order to allow another host to access the metadata.
- **HyperCache-W timeout** – Sets to 480 seconds (8 minutes) by default. Specify the number of seconds the hardware provider should wait for the storage server to flush the HyperCache-W resource when asked to import (create) a SnapshotView. Since this process is potentially time consuming, the maximum setting is 86400 seconds (24 hours).
- **Allow snapshot of mount point volumes** – Enabled by default. When this option is enabled, the agent can determine the volume path information of volumes mounted to directories.
- **Storage Server for import operations** – Sets to Automatic by default. In most cases this option should not be changed. However, if the client is registered to both source and target of a replication pair, specify the storage server to which the hardware provider should send RPCs to for SnapshotView assignment when multiple storage servers are used.

Batch File Options

1. On the **Batch Files** tab, indicate if you want to run batch files before and/or after each snapshot.



In order to run batch files, you must enter an administrative user name and password for the local computer.

You can then click the **Create/Edit** buttons and use Notepad to generate the batch files.

Running the Snapshot Agent

The Snapshot Agent for VSS triggers automatically any time a Snapshot operation occurs on an VTrak S3000 server-managed disk.

To test the Snapshot Agent, take a Snapshot of a virtual drive from the Management Console. Click the **Snapshot** tab to verify that a VSS Snapshot has been created. If the Agent is working corectly, you see **Yes with VSS** in the Quiescent column.

History and Event Logs

Snapshot Agent for VSS history is recorded in the Microsoft Application Event Log as Snapshot Agent events.

Removing Snapshot Agent Software

Use **Add/Remove Programs** from the Control Panel.

Chapter 7: Snapshot Agent for File Systems

- Supported Versions (page 37)
- Installation on Linux (page 37)
- Installation on Windows (page 37)
- Configuring the Snapshot Agent on Windows (page 38)
- Running the File System Agent (page 38)
- Confirming Snapshot Status (page 38)
- Removing the Snapshot Agent Software (page 38)

Snapshot Agents for file systems protect data with full point-in-time consistency while still allowing full speed, almost non-stop access to the data.

Prior to starting the Snapshot process, all disk caches and buffers are flushed to disk.

Using backup software, a back up of the snapshot image can be performed at high speed while the file system operates in normal mode. Because the contents of the snapshot image are guaranteed never to change, what is backed up is consistent, ensuring transactional integrity. While the backup software is reading data from the snapshot image, changes that occur to the data will not affect what gets written. Users are always able to fully access the data while the backup software sees a stable, read-only snapshot image of the data taken an instant before the backup began.

Supported Versions

The Snapshot Agent for File Systems is supported for the following platforms. For specific version information, refer to the Certification Matrix on the www.promise.com website:

- Windows Enterprise Server
- Red Hat Linux Advanced Server

Installation on Linux

Installation of the Snapshot Agent has the following requirements:

- You must be root (or root equivalent) in order to install.
- A SAN Client must be installed.

1. Copy the installation package from the installation media to the local drive of your client.

   Use **/tmp** as an example.
2. Install the Snapshot Agent software.
3. Type the following on Linux:

   rpm -i filesystemagent-<*version number*>-<*build number*>.i386.rp

Installation on Windows

Installation of the Snapshot Agent has the following requirements:

- Before you install the Snapshot Agent, you must install PROMISE SAN Disk Manager (SDM/IMA) on the same machine.

  If SDM/IMA is not detected when Snapshot AgentSnapshot Agent installation begins, an error message displays. Cancel the procedure, install SDM/IMA, and then repeat Snapshot Agent installation.
- You must be an administrator or have administrator privileges in order to install.

1. Launch installation from the installation media.
2. When prompted, enter your license key code.

   The Snapshot Agent license must be registered with PROMISE.
   - If your computer has an Internet connection, the license is activated as soon as you enter your key code and click the **Next** button.
   - If your Internet connection is temporarily down, your license activates automatically the next time the Snapshot Agent is started and your Internet connection is working.
   - If your computer has no Internet connection, you must perform an offline activation. See the *VTrak S3000 Quick Start Guide* for more information.

You have 30 days to activate your license so that you can continue to use the Agent.

3. When done, click **Finish**.

   The File System Agent installs into the same directory as the SDM/IMA.

4. When done, click **Finish**.

   IMA automatically starts the file system agent for you. In addition, IMA automatically starts each time the client is restarted.

Silent Installation

The Snapshot Agent for Windows provides the ability to perform a silent install. A silent install does not require any interaction during the installation process.

In order to install the Snapshot Agent in silent mode, run **setup /s** or **setupsilent.bat**.

Configuring the Snapshot Agent on Windows

By default, no configuration of the Snapshot Agent is required. However, if you are using a service-enabled device (SED) and you have preserved the physical device's inquiry string (set when you create the SED in the Console), you must make a change in the registry.

1. In the registry, locate the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\CurrentVersion\Agents\Agent n

   Agent n is the agent number, that is Agent 1.

   If you have multiple agents installed on the machine, highlight each and check the *Name* field for the one that says *Windows*.

2. Under the correct agent key, add a string (REG_SZ) named **OverRideDrives** and specify the drive letters to which the SED is mounted.

   For example: the value might be E:;F:;

Running the File System Agent

The file system agent triggers automatically any time a Snapshot operation occurs.

To test the file system agent, perform a Snapshot Copy of a virtual drive from the Management Console.

Confirming Snapshot Status

You can get detailed information from the agent trace log. You can find **agttracefs.log** under the IMA installation folder. It is usually installed in **C:\Program Files\IMA**.

Removing the Snapshot Agent Software

Do the following to uninstall the Snapshot Agent software:

Operating System	Commands & Instructions
Windows	You can use Add/Remove Programs from the Control Panel or: 1. Insert the installation media. 2. Choose **Install Products** > **Install Snapshot Agents** > **Install Snapshot Agent for Windows Filesystem** and follow the on-screen instructions.
Linux	Log on to the system as root and remove the client software by executing the following command: rpm -e filesystemagent-<version>-<build> For example: **rpm -e filesystemagent-4.50-904**

Index

A
agent trace log 29, 38
agttracefs.log 38
agttraceU.log 29

B
backup process, ESE 5
backup transaction log 25

C
Command line recovery tool 25

D
data backup and protection 16
database
  MySQL 29
  Oracle 18
database design, virtual device 15
DDL commands 18
diagnostics
  .cab file 1
  log files 1
  X-ray 1

E
ESEUTIL.EXE utility 5
event, appctrl 4
Exchange
  Configure 4
  Install 4
  Introduction 3
  Remove 6
  Run 4
  Snapshot status 4
  Supported versions 3
  verify 4
Exchange Extensible Storage Engine (ESE) 4
Exchange Storage Group 5
Exchange System Manager 3
Exchange Virtual Server 3

F
file system support, Oracle 7
File Systems
  Install
    HP-UX 37
    Linux 37
    Solaris 37
    Windows 37
    Windows silent installation 38
File Systems, cont.
  Remove 38
  Run 38
  Supported versions 31, 37
  Windows Service enabled devices 38
files
  .cab 1
  .his 25
  ExAgent.ini 4
  exchpost.bat 4
  exchpre.bat 4
  MS Exchange Checkpoint 5
fstrace.log file 26

I
ISPurgeExLog utility 5

L
license key code 4, 29
Licensing 21, 33, 37
Log files 1
log files
  agttrace.log 27
  fstrace.log 26
  trace 1
  Windows events 4, 27

M
MS Exchange Checkpoint file 5

O
options
  BackTrak 1
  Replication 1
  Snapshot 1
  Snapshot copy 1
Oracle Archive Logging 14
Oracle Automatic Storage Management (ASM) disks 11

P
platform support
  Snapshot Agent ofr Oracle 7
  Windows Enterprise Server 3, 21

R
recovery scenarios
  Oracle 17

S
SAN Disk Manager 4, 21, 32, 37
SDM/IMA 4
Service enabled devices, Windows 38
Set Agent trace 2
Snapshot Agent
  configure
    Linux 13
    MySQL 29
    Oracle Listener on Windows 11
    Oracle on Windows 9
    SQL Server 22
  install
    Exchange Server 4
    Linux 12
    MySQL 29
    Oracle on Windows 7
    SQL Server 21
  Oracle 14
  remove
    Exchange Server 6
    MySQL 30
    Oracle on Linux 15
    Oracle on Windows 15
    SQL Server 28
  trigger, MySQL 29
Snapshot Agent for Microsoft Exchange 3
Snapshot Copy 4, 14, 27
Snapshot Copy recover, Oracle 17
Snapshot Copy, Oracle 16
Snapshot rollback, Oracle 17
Snapshot status 15
snapshot status, confirm, MySQL 29
Snapshot status, SQL Server 27
Snapshot, Oracle 16
SnapshotView
  Oracle 17
SnapshotView, Oracle 18
SQL Server
  Advanced configuration 25
  Configure 22, 29
  Install 21, 29
    Silent installation 21, 29
  Introduction 21, 29
  Recovering a database 30
  Remove 28, 30
  Run 27, 29
  Supported versions 21, 29
sqlplus utility 14

T
tablespace 15
trace log 1
trace.log
    SQL Server 26

U
utilities
    ESEUTIL.EXE 5
    fsssrest.exe 25
    ISPurgeExLog 5
    Snapshot Agent on SQL Server 22
    sqlplus 14

V
VSS
    Install 32
        Silent installation 33
    Introduction 31
    Remove 35
    Run 35

W
Windows 4
Windows Event log 4

X
X-ray 1